Security and Compliance at U-M

- Do not conflate security and compliance
- Security and compliance are a shared responsibility
- Alignment vs. compliance: do the right thing to the best of your ability
- Using common sense
- It’s a never-ending journey
- Information Assurance is a partner and a resource to you
Today’s Journey

- Why classify data?
- Classification exercises
- Discussion

- Data classification at U-M
- Protecting sensitive data
Why Classify Data

Data classification helps:

➔ Meet legal, regulatory, academic, financial, and operational requirements
➔ Determine minimum security requirements
➔ Take a risk-based approach to data protection
➔ Balance protection of data confidentiality and integrity with the need for collaboration and sharing of knowledge
# U-M Data Classification Levels

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restricted</strong></td>
<td>Disclosure could cause severe harm to individuals and/or the university, including exposure to criminal and civil liability.</td>
<td>Credit card numbers (PCI); FISMA</td>
</tr>
<tr>
<td></td>
<td>Has the most stringent legal or regulatory requirements and requires the most prescriptive security controls.</td>
<td></td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>Disclosure could cause significant harm to individuals and/or the university, including exposure to criminal and civil liability.</td>
<td>HIPAA, CUI, ITAR, SSN, GLBA, etc.</td>
</tr>
<tr>
<td></td>
<td>Usually subject to legal and regulatory requirements due to data that are individually identifiable, highly sensitive, and/or confidential.</td>
<td></td>
</tr>
<tr>
<td><strong>Moderate</strong></td>
<td>Disclosure could cause limited harm to individuals and/or the university with some risk of civil liability.</td>
<td>Building plans, contracts, employee records, FERPA, UMID with names, etc.</td>
</tr>
<tr>
<td></td>
<td>May be subject to contractual agreements or regulatory compliance, or is individually identifiable, confidential, and/or proprietary.</td>
<td></td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>Encompasses public information and data for which disclosure poses little to no risk to individuals and/or the university.</td>
<td>Directory information, public websites, research proposals, course catalogs, UMID w/o names, etc.</td>
</tr>
<tr>
<td></td>
<td>Anyone regardless of institutional affiliation can access without limitation.</td>
<td></td>
</tr>
</tbody>
</table>
The Sensitive Data Guide provides guidance to help make informed decisions about where to safely store and share university data.

It is not intended to be a complete or comprehensive catalog of services available at U-M.

safecomputing.umich.edu/dataguide
Data Classification In Action

Questions to ask:

➔ What type of data is it?
➔ What is the level of sensitivity?
  ◆ Level of harm to individuals
  ◆ Subject to contracts or regulations

[Link to Example: safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/examples-by-level]
Data Classification In Action

Questions to ask:

➔ What type of data is it?
➔ Who does the data concern?
➔ Is it regulated?

THE BIRTH DATE EXERCISE

STAFF
PII: MODERATE
HIPAA: HIGH

PATIENT

STUDENT
FERPA: MODERATE

RESEARCH SUBJECT
HSR: MODERATE

MINOR
COPPA: MODERATE
Data Classification In Action

Questions to ask:

➔ What type of data is it?
➔ What is the purpose of the data?

**CUI**: Controlled Unclassified Information

**FISMA**: Federal Information Security Management Act

---

**CUI vs. FISMA EXERCISE**

- **CUI: HIGH**
- **FISMA: RESTRICTED**

- Government data
  - Use the data for research purposes

- Share with U-M

- Run a service on the government’s behalf

---

**SUMMIT 2020** Reimagined
Data Classification In Action

Security is not the same as compliance

Questions to ask:

➔ What type of data is it?
➔ How is the data collected?
➔ To whom is the data provided?

**PHI**: Protected Health Information (needs BAA)
Protecting Sensitive Data

Sensitive Data must be protected to prevent theft, unauthorized access, compromise, and inappropriate use.

<table>
<thead>
<tr>
<th>Policies and Standards</th>
<th>Minimum Security Requirements</th>
<th>Vendor Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recently revised policy (SPG 601.27) and accompanying information security standards</td>
<td>Organized by information security standard and based on data sensitivity levels</td>
<td>Third Party Vendor Security and Compliance Standard (DS-20) and additional guidance</td>
</tr>
</tbody>
</table>
Policies and Standards

- The U-M Information Security Policy (SPG 601.27) was updated in June 2018.
- It is supported and supplemented by 13 specific operational, procedural, and technical standards.

1. Access, Authorization, and Authentication Management (DS-22)
2. Disaster Recovery Planning and Data Backup for Information Systems and Services (DS-12)
3. Electronic Data Disposal and Media Sanitization (DS-11)
4. Encryption (DS-15)
5. Information Assurance Awareness, Training, and Education (DS-16)
6. Information Security Risk Management (DS-13)
7. Network Security (DS-14)
8. Physical Security (DS-17)
9. Secure Coding and Application Security (DS-18)
10. Security of Enterprise Application Integration (DS-09)
11. Security Log Collection, Analysis, and Retention (DS-19)
12. Third Party Vendor Security and Compliance (DS-20)
13. Vulnerability Management (DS-21)
Security and Compliance at U-M

- Do not conflate security and compliance
- Security and compliance are a shared responsibility
- Alignment vs. compliance: do the right thing to the best of your ability
- Using common sense
- It’s a never-ending journey
- Information Assurance is a partner and a resource to you
Minimum Security Requirements

Available on the [Safe Computing website](http://safecomputingwebsite.com)

### Network Security


Guidance: [Network Security Management](http://networksecuritymanagementwebsite.com)

<table>
<thead>
<tr>
<th>Security Control</th>
<th>Mission Critical?</th>
<th>Restricted</th>
<th>High</th>
<th>Moderate</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement default-deny, least privilege policies on network firewalls</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td></td>
</tr>
<tr>
<td>Isolate trusted networks containing sensitive data from non-trusted networks</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Securely configure network infrastructure devices</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Maintain accurate network documentation</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Document network interconnects to non-U-M parties</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Protect devices not requiring exposure to the internet</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Restrict vendor remote network access to the smallest segment feasible</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Obtain authorization before extending any U-M networks</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Encrypt wireless network traffic</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
</tbody>
</table>
Third Party Vendor Security

- Any external service provider that transmits, stores, or processes university data is considered a third party vendor.
- Follow the Third Party Vendor Security and Compliance Standard (DS-20).
- Additional Guidance is available on the Safe Computing website.

Vendor Assessment Process

1. Engage Procurement Services if possible.
2. Determine Data classification (consult with IA if needed).
3. Based on data classification, the following agreements may be needed:
   - Data Protection Agreement (DPA) or equivalent
   - FERPA Agreement
   - Third Party Security Questionnaire (UMSPSCQ/BTAA or equivalent)
   - Business Associate Agreement (BAA)